2021-09-03

The Development of a Cyber Safety Culture

Hopcraft, Rory

The Development of a Cyber Safety Culture

R. Hopcraft[1*], K. Tam[1], K. Moara-Nkwe[1] and K. Jones[1]
[1]Faculty of Science and Engineering, University of Plymouth, UK
*corresponding author

Abstract – A rise in catastrophic events as a result of poor safety management (e.g. the capsizing of the Herald of Free Enterprise and Costa Concordia), has driven the maritime sector to seek improvements in its safety management. This paper will explore the vital role of the human element within safety management, and why, as part of that safety management companies must foster a safety culture. The development of safety cultures is not new to the maritime sector. However, the increase in connected systems within the sector (e.g. satellite communications etc.) means these safety cultures must now consider the risks posed by digital systems. Therefore, the paper will consider what the core elements of a cyber safety culture are, and how a company can nurture its development. The paper will then conclude by discussing the various benefits of developing a robust cyber safety culture, including demonstrable compliance to the International Maritime Organization's (IMO) cyber regulations, Resolution MSC.428(98).

Keywords
Cybersecurity, safety culture, risk management, Cyber-MAR

Introduction

As a result of various high-profile incidents in the 1980's (e.g. Chernobyl and Herald of Free Enterprise), there was global recognition of the need to develop stringent safety management systems. Throughout the past half century, many sectors, the maritime sector included, have made great strides in developing and enhancing their physical safety management systems (International Transport Forum, 2018).

As a part of this movement, the integration of digital systems into everyday operations has helped to improve safety, as well as efficiency. However, this integration has opened organizations to a new range of safety risks: digital safety systems could be compromised leading to a safety-compromising incident.

Recent terrorist events like September 11th and the USS Cole have raised the issue of security and the threat of outside influence in the maritime sector. The primary reaction was the introduction of the International Ship and Port Facility Security Code by the International Maritime Organization (IMO) in 2004. Recent cyber incidents affecting the maritime sector, most notably the 2017 NotPetya incident that struck shipping giant A.P Møller-Mærsk, also illustrated that digital technology noticeably affects both safety and security. Moreover, it shows the importance of an effective safety culture, and organizational transparency when dealing with these types of incidences.

An organization's safety culture is about more than just addressing safety, security must now be considered as part of it. A robust safety culture must be effective and appropriate to an organizations risk management practices. Allowing the inclusion, and holistic management of, all risks facing an organization and its operations.

Developing a safety culture that is considerate of any new risks is important, as any implemented measures need to be appropriate for the organizations operations, otherwise they will be ineffective. In a new digital and automation filled age, considering cyber security is a priority.

Human error is, and will always be, a large contributor to safety incidents. As such, safety management practices needs to be mindful of the human operators. When establishing and embracing a robust safety culture, organizations can engage with the human element, and ensure they are:

(1) Aware of the risks and how to mitigate them;

(2) Able to make meaningful contributions to the safety of operations.

To explore how, and why, organizations need to develop safety cultures that include cyber this paper will do the following. Firstly, it will explore the role of the human element in safety management. The paper will then discuss what a safety culture is, and ways it they can be created and maintained. The following section will explore the importance of including cyber risk management within an existing safety culture, and the benefits of doing so. Finally, the paper will conclude by discussing how, through engagement with emerging maritime cyber training platforms (e.g. Cyber-MAR), organizations can develop an organization-wide culture that considers cyber risk, operations and personnel holistically.

Safety and the Human Element

In 1986, a series of failures in a safety test led to the explosion of No.4 reactor in the Chernobyl Nuclear Power Plant. An investigation report, released later

that year, argued that human error had been a major contributor to the disaster (International Nuclear Safety Advisory Group, 1986). The initial response of both the company in charge of the power plant, and the Soviet Union were deemed inadequate by the Nuclear Energy Institute (2019). While the specific design of the reactor contributed to the magnitude of the event, the deliberate violation of safety rules coupled with human error were major contributors to the disaster (International Nuclear Safety Advisory Group, 1986). What is more, some of the policies and procedures that should have been in place had not been well articulated (World Nuclear Association, 2021), leaving the operators to make their own interpretations on the best course of action. However, without possessing an adequate understanding of safety, operators were unable to make informed decisions. Thus, operators were negatively affected by the lack of a coherent safety culture/structure.

The year following the Chernobyl disaster, the ferry *Herald of Free Enterprise* capsized shortly after leaving the Belgian port of Zeebrugge. In the inquiry report, Lord Justice Sheen commented that the company from top to bottom was "infected with the disease of sloppiness" (Deparment for Tranport, 1987). The inquiry also noted that proper consideration was not given to the safety system in place, as much required improvement.

These high-profile safety-related incidents helped lead the IMO to openly recognize the importance of the human element in safety. To this end, the IMO adopted *Resolution A.596(15)* which argued for stronger safety management practices on ships (International Maritime Organization, 1988). This work evolved over the following years, and culminated in the adoption of Resolution A.647(16) – *IMO Guidelines on Management for the Safe Operation of Ships and Pollution Prevention (International Maritime Organization, 1989)*. These Guidelines paved the way for the inclusion of the International Safety Management (ISM) Code as a mandatory element of the Safety of Life at Sea Convention (International Maritime Organization, 2020). The adoption of the ISM Code was to ensure all Governments and companies took the necessary steps to ensure the continued safety of maritime personnel (International Maritime Organization, 2014).

As Barnett and Pekcan (2017) argue, in the maritime sector, there is often a complex relationship between safety and the human element. In *Resolution A.947*, the IMO agree that the human element is a complex and multi-dimensional issue that directly affects safety and security. Within which the human element involves "the entire spectrum of human activities performed by ships' crews, shore-based management, regulatory bodies, recognized organizations, shipyards, legislators, and other relevant parties…" (International Maritime Organization, 2003b).

The maritime sector has always been reliant on the people as operators, both on-board ships and within ports. As such, the human element is the center of effective safety management. While digital technology has changed the sector, and the human elements role has changed with it, operations are still reliant on people regardless of how the roles change (Kia, Stayan, & Ghotb, 2000). These socio-technical interactions are both operational, and safety, related.

It is worth noting at this point that the IMO offers a distinct differentiation between safety and security. Safety is defined as protection from injury due to non-intentional events like accidents, and security is protection from intentional events (International Maritime Organization, 2020). This distinction, however, raises concerns when it comes to cyber security and the development of a cyber safety culture, as cyber risk management should be about both safety and security events.

As argued by the International Atomic Energy Agency, the management of safety and security often occurs at the same time (International Atomic Energy Agency, 2020). As such, organizations will deal with the consequences of an incident in the same way, regardless of its initial cause. For instance, if this thinking were adopted into the maritime sector, the initial and often instinctual response of the crew will likely be the same to a failure of the electronic navigation systems, regardless whether the cause of the outage was a power failure, or a cyber-attack. Here the human element continues to be a fundamental part of ensuing safety and security through adequate cyber risk management practices.

However, Singleton (1973) argues that the cause of most safety-related incidents can be traced back to inadequate training, instruction or attention. From Verizon's (2020) recent Data Breach report, 20% of reported breaches were caused by human error. This has led to the human element sometimes being referred to as the biggest internal threat facing the cyber security of companies (Boletsis, Halvorsrud, J B Pickering, & Surridge, 2021; Meshkat, Miller, Hillsgrove, & King, 2020). Findings from BIMCO latest cyber security whitepaper highlights that there is a general perception in the sector that humans are the weak link in the cyber risk management chain. 52% of respondents identified people as their company's biggest cybersecurity vulnerability (IHS Markit, 2020).

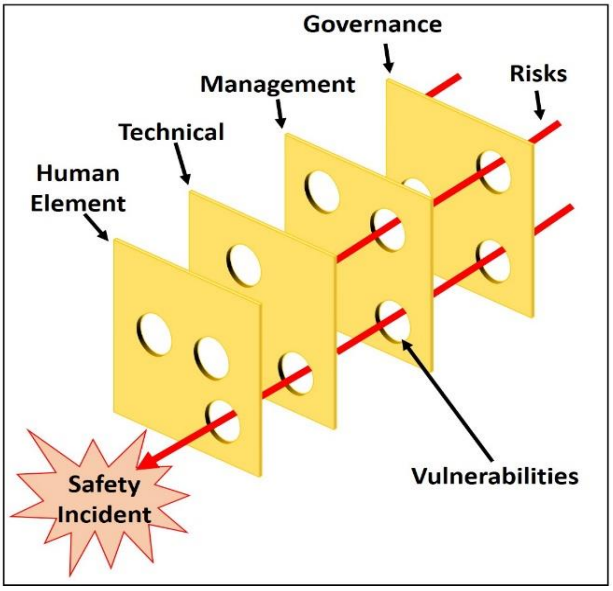

Figure 1. Maritime Safety Swiss Cheese Model

As operators, the human element is often responsible for ensuring work-related systems remain operational. As highlighted by Barnett and Pekcan (2017) the operators of a system often form the last barrier within a cyber risk management system. Following Reason's (1997) *Swiss Cheese Model*, cyber risk management relies on the development of different layers of mitigations (see Figure **1** for example). These mitigations can include hardware, software or policies and procedures. However, like its namesake, these layers have weaknesses (holes) in them.

The aim of an effective cyber risk management system is to ensure those holes do not align and the whole is safer than individual layers. As one layer of defense, it is important that the human element is able to make decisions that do not introduce vulnerabilities to the model, and mitigate the risks from adjacent layers. An example would be writing a password on a post-it note and attaching it to the terminal it is used to login with. Here, the technical mitigation is passwords, yet the human element has introduced a weakness by writing the password down for all to see.

Table 2 illustrates how failures at the different layers of the Swiss Cheese Model led to the capsizing of the Herald of Zeeburgge. It is important to note that in isolation none of these failures would have led to the catastrophic event. However, when coupled together a risk penetrated the layers of mitigations allowing a safety incident to occur.

Humans, as the operators or custodians of digital systems play a vital role in ensuring they do not compromise the safety of those systems. The human element must be aware of the safety risks during operations, and appropriate management practices ensure that a company's safety management system is not eroded.

Elements of a Cyber Safety Culture

To understand what a cyber safety culture is, we must first consider the definition of a safety culture. The initial Chernobyl disaster report attributed many of the failings to the lack of a safety culture locally within the power plant. This led to safety being treated as low priority by personnel or the organization. Over the ensuing years, the organization responsible for that report, the International Atomic Energy Agency (IAEA), have led the way in developing the definition of a safety culture.

> "Safety culture is that assembly of characteristics and attitudes in organizations and individuals which establishes that, as an overriding priority, nuclear power plant safety issues receive the attention warranted by their significance." International Nuclear Safety Advisory Group (1991).

While now dated, this was a critical point in history which still affects decisions today, and the definition given above still remains relevant today, arguing that, within an organization, safety should be understood to be, and is accepted as, the number one priority (International Nuclear Safety Advisory Group, 1996). For safety to be seen as a high priority it requires the engagement with the human element. This engagement includes the awareness, support and accountability for safety on the part of all individuals within an organization (Corrigan, Kay, Ryan, Ward, & Brazil, 2019).

The IMO, due to its engagement with the human element as the focal point of safety, has a long history

Table 1. Factors Leading to the Capsize of the Herald of Free Enterprise

Failure in…			
Governance	**Management**	**Technical**	**Human Element**
Bow and stern loading doors were only required to be weathertight (a lesser watertightness level).	Memorandum sent to operators pressuring them to load and leave Zeeburgge 15mins ahead of schedule.	Lack of fool proof system to indicate to bridge that the doors have been closed.	The Captain accelerated rapidly, causing water to flood the car deck.

of promoting the development of safety cultures. The release of IMO *Resolution A.947(23),* in 2003 continues to draw the link between safety and the human element. As such, companies should be developing "a framework for understanding the complex system of interrelated human element factors, incorporating operational objectives, personal endurance concerns, organizational policies and practice… in order to facilitate the identification and management of risk factors in a holistic and systematic manner" (International Maritime Organization, 2003b).

The increase in digital technology in the maritime sector has led to a changed relationship between the human element and safety. Many of these digital systems boast benefits like improved efficiency while make operations safer. However, risks arise from ill-structured or mismanaged interactions between man and machine (Pidgeon & O'Leary, 2000). For instance, human stress, and the resulting errors, can also be an effect of embracing technology like automation (Tam, Hopcraft, Crichton, & Jones, 2021).

Coined by Emery and Trist (1960), the term most used to describe these systems of interactions between man and machines is socio-technical systems. As Davis, Challenger, Jayewardene, and Clegg (2014) illustrates, there are six different elements within these systems: goals, people, infrastructure, technology, culture and procedures. Each of these elements can have an influence on safety.

Baxter and Sommerville (2011) surmise that a socio-technical system has these individual but interdependent technical and social parts. Furthermore, they argue that system performance relies on the joint optimization of both these parts. Solely focusing on one, to the exclusion of the other is likely to lead to poor performance and increase risks. Therefore, the development of a safety culture must consider the influence and interactions of both equally. For example, if operational goals are set too high, personnel may cut corners to ensure they are on target, at the detriment of safety. Conversely, if the technological solution is too cumbersome, personnel may find work-rounds that again affect safety. If these are developed in collaboration instances of deliberate violations should be reduced.

As Figure 1 illustrates, there are multiple layers found within a socio-technical maritime safety system. Firstly, the governance layer, which represents the regulations and laws companies, must abide by. The second layer is the management layer, which is the internal policies and practices that govern a company's specific risk profile. The third layer is the technical layer. This layer comprises the technical and often digital safety management and mitigation systems. The final layer within the maritime safety system is the human element, and as discussed this layer is responsible for operating within the safety constraints of the company. A strong safety culture encompasses all these layers. As such, a company should create safety management practices that are considerate of the company-specific risks, whilst ensuring all the layers remain aligned.

In 2003, the United Kingdom submitted MSC.77/17 to the IMO. This document argued that while the ISM Code stipulated the need to develop a safety culture, it did little in the way to define what this meant. The aforementioned document goes on to define a safety culture as "a culture in which there is considerable informed endeavor to reduce risks to the individual, ships and marine environment to a level that is 'as low as is reasonably practicable" (International Maritime Organization, 2003a).

As noted by Berg (2013), faults in organizational structures, like those found within the company responsible for operating Chernobyl, have contributed to various safety-related incidents. These behaviors are demonstrated by the two categories of failures outlined by Barnett and Pekcan (2017). The first is "active" failures, where the human element lack the required skills to operate safely. The second cause are "latent" failures, where there are ingrained weaknesses within the organization, possibly within the structure, or safety management system itself, that led to a safety incident occurring. Thus, to reduce risk to the lowest level practicable a safety culture requires an attitudinal change in personnel as well as an organizational change in its approach to safety. Considering the failures listed in Table 1 the active failure would be the crew's unsafe operation of the bow doors. The latent failure would be the management's insistence for early departures.

It is important to note that within the literature there is often a distinction between a safety culture, a cyber security culture and an information security culture. In their detailed analysis of information security cultures Veiga, Astakhova, Botha, and Herslemann (2020) offer two clear definitions. A cybersecurity culture "relates to the manner in which people perceive cybersecurity and the resultant behavior in cyberspace that impacts on the protection of the digital information, systems and people". Whereas an information security culture focuses on the way in which personnel processes information and how this has an impact on its protection.

Individually these definitions do not cover the full concept of a cyber safety culture within a socio-technical system. The cyber security culture

definition limits the behaviors to personnel within the company, and fails to address those externally aiming to do harm. The information security culture is limited to the information. From the understanding that safety cultures must be developed from within a socio-technical framework, these definitions do little to incorporate the multifaceted relationships between the various elements of a socio-technical system.

These definitions also do not address the risks that operations pose to the safety of digital systems. For example, extreme weather, like ice or fog can have a detrimental impact on digital systems. These operational factors pose risks to safety, and have nothing to do with the human element, aside from the fact that they are expected to continue to operate safely when these systems are compromised.

As discussed above, to address the complexities of safety management the IMO ratified the ISM Code. One of the primary aims of the ISM Code is to ensure companies develop, implement, and maintain a safety management system. The application of the SMS is to encourage the development of a safety culture within the company (International Maritime Organization, 2013).

Remembering, that while the IMO define safety and security differently, they use cyber risk as an all-inclusive term, for both safety and security related events. The release of *Resolution MSC.428(98)* marked this change, with the stipulation that company's include cyber risk within their safety management practices (International Maritime Organization, 2017). These cyber risks must include both accidental and deliberate events. Whereby, cyber risk refers to a "measure of the extent to which a technology asset could be threatened by a potential circumstance or event, which may result in shipping-related operational, safety or security failures…" (International Maritime Organization, 2021). Thus, companies, as part of their risk management processes, should be developing a safety culture that includes the identification, and assessment and mitigation of cyber threats, regardless of intentionality.

Summarizing and adapting our earlier definitions, a cyber safety culture is a collection of characteristics and attributes that endeavors to reduce cyber risks to a level that is as low as reasonably practicable. To do this, organizations' should be considering the impact of their internal practices and infrastructures on personnel behaviors. Ensuring that these elements do not led to situations where safety violations occur.

Developing a Cyber Safety Culture

In his review of Australian cyber security culture initiatives, Alshaikh (2020) argues that little is known about how organizations can develop an effective cyber security culture. However, in an industrial sector like the maritime, where safety management has had time to gain traction, lessons can be learnt.

As discussed above, the human element is an inherent factor of risk in the maritime sector, and as such cannot be totally removed from operations. However, through methods such as good management policies, effective training, and the attainment of suitable qualifications and experience these risks can be reduced (Berg, 2013). Thus, the primary goal of the ISM Code, and the SMS, is to achieve peak safety performance, where there are no operational incidents, no personal injuries, and no harm to the environment. To achieve this, organizations' must develop a close relationship between their safety culture and their SMS (American Bureau of Shipping, 2016).

The preamble to the ISM Code reiterates that safety requires commitment from all levels of an organization (International Maritime Organization, 2014). This includes the development of competencies, attitudes and motivations towards safety. However, while the ISM Code provides a framework for understanding safety, and the role of a safety culture, an effective safety culture must go beyond mere compliance to the ISM Code (Corrigan et al., 2019), and must be embedded in every operation.

The development of an effective safety culture must often overcome several fundamental barriers within an organization (Pidgeon & O'Leary, 2000). The first of which are information difficulties. These difficulties often stem from the misunderstanding of complex digital systems and their risks. In this sense, risks may be misunderstood, or go unnoticed, as they span numerous facets of an organization. Other difficulties arise from when the safety incident differs from the predicted event outlined in the SMS, such that personnel must consider actions that are not predetermined by the safety management system. These decisions must be made rapidly, and often without all the required information.

The second set of difficulties that Pidgeon and O'Leary (2000) highlight, are organizational behaviors. They argue that the power dynamic between the regulator and regulated often undermines safety actions, as the regulated do not see the benefits of cumbersome safety processes. Furthermore, because of this power dynamic individuals may feel pressured to not report incidents or failings in the safety system as this could result in bad publicity for the organization, or punishment for operators. Hence, the drive for the inclusion of management in the development of safety management practices would mitigate that issue.

Figure 3. Safety Culture Pyramid - Adapted from Drouin (2010)

From their extensive review on safety cultures Zhang, Wiegmann, Thaden, Sharma, and Mitchell (2002) outline the following common features of a successful safety culture. All these commonalities help overcome some of the challenges facing safety culture development. Firstly, safety cultures are a concept defined at a group level i.e. at an Organization level. Secondly, they are developed through the contribution of all individuals within the Organization. Thirdly, once developed these safety cultures a relatively enduring, stable and somewhat adaptable to change.

In his short introduction to safety cultures, Drouin (2010) outlines the core elements of development within a safety culture (see Figure 2). This pyramid highlights some key lessons on the development of a safety culture.

Firstly, while there must be engagement from all levels of the organization, the shore-based leadership (as seen on the bottom of Figure 2) is the fundamental foundation of an organization's safety culture. It is the responsibility of leaders to engage broadly with risk management practices, including engagement with outside sources of expertise to inform their understanding of risk. These leaders are then responsible for synthesizing this understanding with the day-to-day operational requirements of their organization, to ensure appropriate risk management practices are developed at each level (e.g. crew)

Secondly, even those at the top of the pyramid who are most removed from the overall decision-making process, but probably more exposed to the risks, have responsibilities in the development of the safety culture. Operational personnel at this level still have a responsibility to engage with risk management practices, while also contributing to the improvement of those practices.

What is interesting with Drouin's pyramid is the inclusion of shipboard leaders. These individuals, like their shore-based counterparts, have a responsibility to understand the risk management practices. Due to the isolating nature of maritime operations, these leaders are also responsible, and expected, to make safety decisions in time critical situations. Moreover, they are also responsible for motivating and instructing the personnel they oversee, ensuring they are complying to risk management practices.

Thus, if we apply this pyramid logic to the earlier model of risk management, it becomes apparent that each of those mitigation layers consists of their own layers (see Figure 3). For instance within the human element layer consists of a crew, a shipboard leaders and a shore-based leaders layer. Each of these layers have their own understandings of risks and their own responsibilities to manage risk. Therefore, the vulnerabilities found in the human element layer constitutes a combination of these sub-layers. What is more, each of the mitigation layers will consist of their own sub-layers. Making it important to understand how these interact and inform risk management practices within a safety culture.

While the pyramid illustration does little to represent the communication flows within an organization, the placement of the risk management objectives in the middle does. The risk management objectives should be developed with the input from all levels of the Organization. The lessons learnt from those on the operational frontline should be fed into the objectives

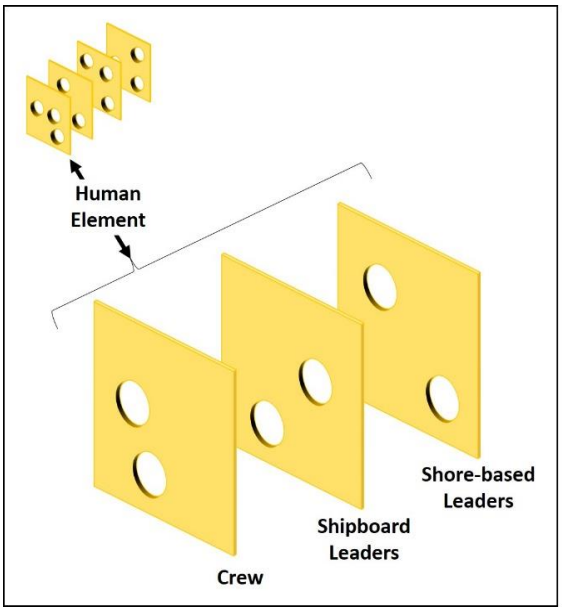

Figure 2. Sub-Layers Within Maritime Mitigation

development, just as the knowledge gained by the leadership should also inform the development.

While the safety culture pyramid illustrates the importance of organizational structure and the roles they have within the development of a safety culture, it does not address the behaviors and attitudes of individuals across the organization. As reiterated by Alshaikh (2020), the development in cybersecurity behaviors has a significant impact on the process from compliance to culture.

Since the terrorist attacks on September 11th 2001, the aviation sector, like the maritime sector, has been keenly motivated to demonstrate their commitment to improving operational safety and security. As such the US Federal Aviation Administration argue that a positive safety culture is built upon five behavioral principles: informed culture, flexible culture, reporting culture, learning culture and a just culture (Quezadra, 2016).

An informed culture ensures personnel are knowledgeable about the human, technical and Organizational factors that determine safety. A flexible culture allows personnel to adapt Organizational process when facing certain kinds of risks, especially those that are unexpected. A reporting culture goes hand-in-hand with a just culture, where personnel are prepared to report their errors without fear of reprisal. Finally, a learning culture is demonstrated when people have a willingness and the competence to draw conclusions from safety information systems.

This idea of a just culture has been recognized as an important attitudinal change within the maritime sector. The IMO (2011) argue that a just culture is founded on two principles: 1) human error is inevitable, and, 2) everyone is accountable for their actions if they knowingly violate safety procedures. A just culture therefore should not punish people for genuine mistakes. With management actively engaging, and encouraging others to step forward, it allows lessons to be learnt from mistakes and development to occur. What is more, this managerial investment ensures personnel feel empowered to come forward, discus risk, and have an invested interest in the development of better risk management practices.

As one of the largest Classification Societies, representing 18% of the world's fleet, the American Bureau of Shipping (ABS) are key drivers in the development of a safety culture within the maritime sector (American Bureau of Shipping, 2019). To see these improvements organizations must identify areas of strength, weaknesses in defenses and opportunities for improvement against incidents (American Bureau of Shipping, 2014). As such, ABS have developed the core safety features they believe need to be present, and enhanced to ensure the development of an effective safety culture (see Table 2).

Within the maritime sector there is ongoing research assessing the usefulness of many tools for testing and nurturing a cyber safety culture. Many of these tools involve the use of simulated environments as a representation of an organization's digital systems. These simulated environments allow organizations to develop and test their cyber risk management practices safely (Priyadarshini, 2018). One such tool is the Cyber-MAR platform, aiming to provide a knowledge-based tool through which companies can better understand their cyber risks (Cyber-MAR, 2019). This understanding will then allow companies to develop and nurture cyber risk management

Table 2. Core safety factors of an effective safety culture – Adapted from American Bureau of Shipping (2014)

Safety Factor	Definition
Communication	Vertical and horizontal communications channels are open and effective.
Empowerment	Individuals feel empowered to fulfil their safety requirements, which are clearly defined by the organisation.
Feedback	Priority is placed on the communication and response to safety issues and concerns
Mutual Trust	Individuals trust that managers do the right thing to support safety, and take on their responsibilities
Problem Identification	All individuals has experience and training to recognise unsafe acts and take avoidance measures.
Promotion of Safety	Management lead the way in promoting safety as a core value to the organisation. Not just seen as a for-profit exercise.
Responsiveness	Individuals are responsive to the demands of their hobs, including unexpected events and emergencies.
Safety Awareness	All individuals have a strong awareness of their responsibilities for their safety, safety of co-workers, organisation and environment.

practices that enhance the core safety factors as outlined by ABS.

Benefits of a Cyber Safety Culture

With the ratification of MSC.428(98), as of January 1st 2021 a company's SMS must now consider cyber risk management. The inclusion of cyber risk into the SMS ensures that there is a commitment its effective management and is not merely a 'paper exercise'. Without the inclusion of cyber in the SMS there is a risk that in a complex organization that safety management becomes inconsistent, under-resourced and not business driven (Gordon, Perrin, & Kirwin, 2007). Successfully developing a safety culture that is considerate of cyber risk will have many benefits to an organization.

Firstly, a successful cyber safety culture must provide demonstrable understanding of cyber risk to ensure compliance with Resolution MSC.428(98). The US Coast Guard's Work Instruction *CVC-WI-027* argues that if under questioning crew are not able to demonstrate a general level of cyber risk management this could constitute a failure of the SMS, leading to detention of the ship (United States Coast Guard, 2020). As such, due to the hierarchical nature of command on-board, safety considerations depend upon the actions of the master and officers (Räisänen, 2009). The development of a cyber safety culture ensure that these personnel are able to make informed decisions about safety. Furthermore, the encouragement of a cyber safety culture that encourages the empowerment of all personnel will allow lower ranking crew to feel comfortable discussing safety practices with superiors (Drouin, 2010). A process that actively strengthening the safety culture throughout the organization.

Secondly, the development of an effective cyber safety culture will reduce the risk that the human element pose to safety, and allow employees to "become robust human firewalls" against cyber incidents (European Union Agency for Network and Information Security, 2017). The strengthening of the human element will have a significant impact on cyber risk management across the organization. As illustrated by the 2017 NotPetya incident at A.P Møller-Mærsk, the consequences of a cyber incident can be non-trivial. While events of this scale are rare, and the likelihood of the human element being able to stop them is low, they illustrate that if personnel are prepared for these events they may make decisions that limit the incidents impacts. The incident destroyed 55,000 computers and 7,000 servers (Ashford, 2019). Costing the company around $40million to recover (A.P Møller-Mærsk, 2019).

Thirdly, the improvement of a company's cyber safety culture will also help to avoid other financial implications like regulatory fines or reputational damage. If doing business within Europe, companies must comply with the EU's General Data Protection Regulation. Failure to ensure adequate date security could lead to a hefty fine of €20million or 4% of global turnover. The 2018 British Airways data breach, that affected over 380,000 transactions (BBC, 2018), illustrates the consequences of poor data protection. While the final fine was reduced because of the global pandemic, the initial fine was expected to be around £183.39million (Information Commissioner's Office, 2020). The negative publicity from these types of incidents, and their handling often damages a company's reputation. Consequently, there can be a fall in customer or investor confidence, which ultimately has an impact on the financial stability of the company. Through the improvement of a cyber safety culture a company is more aware of the risks digital technology poses to its data, and its personnel are better prepared to mitigate those risks. A company that implements a high-level of cyber security, can in the event of a major incident, assure customers that cyber security is taken seriously. Thus, helping to mitigate some of the negative implications of the incident.

The final benefit of a developed cyber safety culture that this paper explores is the reduction in insurance premiums. Many of the Classification Societies, who are responsible for ensuring ships are up to code, have now introduced some form of cyber notation (e.g. Lloyd's Register's CyberSAFE notation). The notation acts as verification that a ship, and its crews, are managing cyber risk adequately on-board. This notation can then be used as proof with insurers to illustrate the company are 1) compliant with current international regulations, 2) aware of their cyber risks, and 3) have adequate safeguards in place to mitigate those risk. This reduction in risk means they could be offered better insurance premiums because they likelihood of a cyber-incident occurring is reduced. Furthermore, as the US Coast Guard illustrates in its enforcement of MSC.428(98), being able to show appropriate cyber risk management practices also demonstrates compliance.

Conclusion

This paper has presented evidence that safety cultures are a fundamental part of maritime risk management. With more digital systems being integrated onto every ship and into very operations, crew safety is becoming more reliant upon those systems. It is then no surprise that safety cultures should now include cyber risks. However, as seen with other risks, it takes time for these cultures to develop and establish (Parker, Lawrie, & Hudson, 2006). This paper has explored various ways in which companies can facilitate the development of their cyber safety

cultures. One such platform is the CyberMAR project. The platform offers a sector-specific environment, helping companies understand their cyber risk management and develop their safety cultures.

However, it is important to conclude that the development of a cyber safety culture will not make a company immune to all risk. A quick look at the news headlines will highlight that accidents still happen, but they are just that, accidents. Not only that, but the few times incidents do happen, response and recovery is much quicker as the organization and its personnel are better informed about these risks. The primary aim of a safety culture is to stop events, like the sinking of the Costa Concordia, due to deliberate negligence or poor decision-making from happening (The Guardian, 2013), and reduce the impacts of accidents that unfortunately do happen.

Acknowledgements

This paper is a partly funded by the research efforts under Cyber-MAR. Cyber-MAR project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 833389. Content reflects only the authors' view and European Commission is not responsible for any use that may be made of the information it contains.

References

A.P Møller-Mærsk. (2019). *Cyber Security in the Maritime Sector*. Paper presented at the International Maritime Organization - Maritime Safety Committee 101, London.

Alshaikh, M. (2020). Developing cybersecurity cutlure to influence employee behavior: A practice perspectice. *Computers & Security, 98*, 1-10. Retrieved from https://doi.org/10.1016/j.cose.2020.102003

American Bureau of Shipping. (2014). *Safety Culture and Leading Indicators of Safety*. Retrieved May 11th, 2021, from https://maritimesafetyinnovationlab.org/wp-content/uploads/2016/03/abs-safety-culture-and-leading-indicators-of-safety.pdf

American Bureau of Shipping. (2016). *Ergonomic & Safety Discussion Paper*. Retrieved May 12th, 2021, from https://ww2.eagle.org/content/dam/eagle/innovation-and-technology/safety-and-human-factors/Discussion-Paper-MSRI-Safety-Culture.pdf

American Bureau of Shipping. (2019). *Annual Review 2019*. Retrieved 20th May, 2021, from https://ww2.eagle.org/content/dam/eagle/publications/annual-review/ABS-Annual-Review-2019.pdf

Ashford, W. (2019). NotPetya offers industry-wide lessons, says Maersk's tech chief. Retrieved 21st April, 2021, from ComputerWeekly.com: https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief

Barnett, M. L., & Pekcan, C. H. (2017). The Human Element in Shipping. In *Encyclopedia of Maritime and Offshore Engineering* (pp. 1-10): Wiley Online.

Baxter, G., & Sommerville, I. (2011). Socio-technical systems: From deisgn methods to systems engineering. *Interacting with Computers, 23*(1), 4-17. Retrieved from https://doi.org/10.1016/j.intcom.2010.07.003

BBC. (2018). BA investigation into website hack reveals more victims. Retrieved October 25, from https://www.bbc.co.uk/news/technology-45953237

Berg, H. P. (2013). Human Factors and Safety Culture in Maritime Safety. *TransNav, 7*(3), 343-353. doi:10.12716/1001.07.03.04

Boletsis, C., Halvorsrud, R., J B Pickering, S. P., & Surridge, M. (2021). *Cybersecurity for SMEs: Introducing the Human Element into Socio-tehnical Cybersecurity Risk Assessment.* Paper presented at the Poceedings of the 16th International Joint Conference on Computer Vision, Imaging and Computer Graphics Theory and Applications.

Corrigan, S., Kay, A., Ryan, M., Ward, M. E., & Brazil, B. (2019). Human factors and safety culture: Challenges and opportunities for the port. *Safety Sci, 119*, 252-265. Retrieved from https://doi.org/10.1016/j.ssci.2018.03.008

Cyber-MAR. (2019). Cyber-MAR Fact Sheet. Retrieved from https://www.cyber-mar.eu/wp-content/uploads/2019/12/Cyber-MAR_Fact-sheet_v.4.pdf

Davis, M. C., Challenger, R., Jayewardene, D. N. W., & Clegg, C. W. (2014). Advancing socio-technical systems thinking: A call for bravery. *Applied Ergonomics, 45*, 171-180. Retrieved from http://dx.doi.org/10.1016/j.apergo.2013.02.009

Deparment for Tranport. (1987). *Herald of Free Enterprose Formal Investigation*. Retrieved May 10th, 2021, from https://assets.publishing.service.gov.uk/media/54c1704ce5274a15b6000025/FormalInvestigation_HeraldofFreeEnterprise-MSA1894.pdf

Drouin, P. (2010). The building blocks of a saafety culture. *Seaways, October*, 4-7. Retrieved from http://www.safeship.ca/uploads/3/4/4/9/34499158/safety_culture_pauldrouin.pdf

Emery, F. E., & Trist, E. L. (1960). Socio-technical systems. In C. W. Churchman & M. Verhulst (Eds.),

Management Science Models and Techniques (Vol. 2, pp. 83-97). Oxford: Pergamon.

European Union Agency for Network and Information Security. (2017). *Cyber Security Culture in Organisations*. Retrieved 19th May, 2021, from https://www.enisa.europa.eu/publications/cyber-security-culture-in-organisations

Gordon, R., Perrin, E., & Kirwin, B. (2007). Measuring safety culture in a reaserch and development centre: a compaison of two methods in the Air Traffic Management domain. *Safety Sci, 45*(6), 669-695. Retrieved from http://dx.doi.org/10.1016/j.ssci.2007.04.004

IHS Markit. (2020). *Safety at Sea and BIMCO cyber security white paper*. Retrieved 10th May, 2021, from https://ihsmarkit.com/Info/0819/cyber-security-survey.html

Information Commissioner's Office. (2020). *Penalty Notice - British Airways*. Retrieved from

International Atomic Energy Agency. (2020). *Safety Culture Practices for the Regulatory Body*. Retrieved 16th May, 2021, from https://www-pub.iaea.org/MTCD/Publications/PDF/

International Maritime Organization. (1988). *Resolution A.596(15) - Safety of Passenger Ro-Ro Ferries*. London: International Maritime Organization

International Maritime Organization. (1989). *Resolution A.647(16) - IMO Guidelines on Management for the Safe Operation of Ships and Pollution Prevention*. London: International Maritime Organization

International Maritime Organization. (2003a). *MSC.77/17 - Role of the Human Element*. London: International Maritime Organization

International Maritime Organization. (2003b). *Resolution A.947(23) - Human Element Vision, Principles and Golas for the Organization*. London: International Maritime Organization

International Maritime Organization. (2011). *MEPC 62/17/2 - Human and Organizational Factors - The Critical Role of "Just Culture"*. London: International Maritime Organization

International Maritime Organization. (2013). *MSC-MEPC.7/Circ.8 - Revised Guidelines for the Operational Implementation of the International Safety Management (ISM) Code by Companies*. London: International Maritime Organization

International Maritime Organization. (2014). *International Management Code for the Safe Operation of Ships and for Pollution Prevention*. London: Internation Maritime Organization.

International Maritime Organization. (2017). *Resolution MSC.428(98) Maritime Cyber Risk Management in Safety Management Systems*. London: International Maritime Organization

International Maritime Organization. (2020). *International Convention for the Safety of Life at Sea*. London: International Maritime Organization.

International Maritime Organization. (2021). Maritime Cyber Risk. Retrieved from https://www.imo.org/en/OurWork/Security/Pages/Cyber-security.aspx

International Nuclear Safety Advisory Group. (1986). *INSAG-1 - Summary report on the Post-accident Review Meeting on the Chernobyl Accident*. Retrieved 9th May, 2021, from https://www.iaea.org/publications/3598/summary-report-on-the-post-accident-review-meeting-on-the-chernobyl-accident

International Nuclear Safety Advisory Group. (1991). *Safety Series No.75-INSAG-4 - Safety Culture*. Retrieved 9th May, 2021, from https://www-pub.iaea.org/MTCD/publications/PDF/Pub882_web.pdf

International Nuclear Safety Advisory Group. (1996). *Report on Defence in Depth in Nuclear Safety*. Retrieved 10th May, 2021, from https://www-pub.iaea.org/MTCD/publications/PDF/Pub1013e_web.pdf

International Transport Forum. (2018). *Safety Management Systems*. Retrieved 25th June, 2021, from Paris: https://www.itf-oecd.org/sites/default/files/docs/safety-management-systems.pdf

Kia, M., Stayan, E., & Ghotb, F. (2000). The Importance of Information technology in port terminal operations. *International Journal of Physical & Logistics Management, 30*(3/4), 221-344. doi:10.1108/09600030010326118

Meshkat, L., Miller, R. L., Hillsgrove, C., & King, J. (2020). *Behavior Modeling for Cybersecurity*. Paper presented at the 2020 Annual Reliability and Maintainability Symposium (RAMS).

Nuclear Energy Institute. (2019). Chernobyl Accident and Its Consequences [Press release]. Retrieved from https://www.nei.org/resources/fact-sheets/chernobyl-accident-and-its-consequences#:~:text=Key%20Facts,design%2C%20combined%20with%20human%20error.

Parker, D., Lawrie, M., & Hudson, P. (2006). A framework for understanding the development of orgniasational safety culture. *Safety Culture, 44*, 551-562. doi:10.1016/j.ssci.2005.10.004

Pidgeon, N., & O'Leary, M. (2000). Man-made disasters: why technology and organizations (sometimes) fail. *Safety Science*, *34*(1), 15-30. doi:https://doi.org/10.1016/S0925-7535(00)00004-7

Priyadarshini, I. (2018). *Features and Architecture of The Modern Cyber Range: A Qualitative Analysis and Survey*.

Quezadra, R. D. L. (2016). *Introduction to "Just Culture"*. Paper presented at the ATS Incident Analysis Workshop.

Räisänen, P. (2009). *Influence of Corporate Top Management to Safety Culture - A Literature Survey*. Turku University of Applied Sciences, Retrieved from https://www.merikotka.fi/wp-content/uploads/2018/08/isbn9789522161048.pdf

Reason, J. (1997). *Managing the Risks of Organisational Accidents*. Aldershot: Ashgate Publishing.

Singleton, W. T. (1973). Theoretical Approaches to Human Error. *Ergonomics*, *16*(6), 727-737. doi:10.1080/00140137308924563

Tam, K., Hopcraft, R., Crichton, T., & Jones, K. (2021). The potential mental health effects of remote control in an autonomous maritime world. *Journal of International Maritime Safety, Environmental Affairs, and Shipping*, *5*(2), 51-66. doi:10.1080/25725084.2021.1922148

The Guardian. (2013). Five Costa Concordia staff convicted over shipwreck in Italy. Retrieved 24th May, 2021, from https://www.theguardian.com/world/2013/jul/20/five-costa-concordia-guilty-shipwreck-italy

United States Coast Guard. (2020). *CVC-WI-027(1) - Vessel Cyber Risk Management Work Instruction*. Retrieved from

Veiga, A. d., Astakhova, L. V., Botha, A., & Herslemann, M. (2020). Defining organisaational information security culture - Perspectives from academia and industry. *Computers & Security*, *92*(May), 1-23. Retrieved from https://doi.org/10.1016/j.cose.2020.101713

Verizon. (2020). *2020 Data Breach Investigations Report*. Retrieved 20th May, 2021, from https://enterprise.verizon.com/content/verizonenterprise/us/en/index/resources/reports/2020-data-breach-investigations-report.pdf

World Nuclear Association. (2021). Chernobyl Accident 1986 [Press release]. Retrieved from https://www.world-nuclear.org/information-library/safety-and-security/safety-of-plants/chernobyl-accident.aspx

Zhang, H., Wiegmann, A., Thaden, T. l. v., Sharma, G., & Mitchell, A. A. (2002). *Safety Culture: A Concept in Chaos?* Paper presented at the 46th Annual Meeting of the Human Factors and Ergonomics Society, Sanat Monica.